

## MicroPatent® PatSearch Fulltext: Record 1 of 1

**Search scope:** JP (bibliographic data only)

**Years:** 1836-2006

**Patent/Publication No.:** ((JP2002207739))



[Go to first matching text](#)

### JP2002207739 A DOCUMENT MANAGEMENT SYSTEM NS SOLUTIONS CORP

#### Abstract:

**PROBLEM TO BE SOLVED:** To allow the quick access to a necessary document when required and surely limit the access according various security levels. **SOLUTION:** An access control list shown in Fig.2 plays a central play in the limitation of the access to the document. One line of the access control list is formed of a plurality of fields described in the top line of each row. The information of each field included in one line (record) is the whole information required to set a prescribed access limit to a document containing a certain character line. The 'character line' field means that the document containing the character line described in this field is the document to be limited for access of a number of documents accumulated in a database.

ID	文字列	許可回数	許可レベル	有効期限	有効期間終了日
1001	1001	1001	1001	2002/06/30	1
1002	1002	1002	1002	2002/06/30	1
1003	1003	1003	1003	2002/06/30	1
1004	1004	1004	1004	2002/06/30	6
1005	1005	1005	1005	2002/06/30	6

[Click here for larger image.](#)

#### Inventor(s):

SHIMOMURA OSAMU  
SAKAI SHUSUKE

**Application No.** 2001004843 JP2001004843 JP, **Filed** 20010112, A1  
**Published** 20020726

**Original IPC(1-7):** G06F01730  
G06F01214

**Patents Citing This One** No US, EP, or WO patent/search reports have cited this patent.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-207739

(P2002-207739A)

(43) 公開日 平成14年7月26日 (2002.7.26)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード (参考)
G 0 6 F 17/30	1 2 0	G 0 6 F 17/30	1 2 0 B 5 B 0 1 7
12/14	3 1 0	12/14	3 1 0 K 5 B 0 7 5

審査請求 未請求 請求項の数6 OL (全 9 頁)

(21) 出願番号 特願2001-4843 (P2001-4843)

(22) 出願日 平成13年1月12日 (2001.1.12)

(71) 出願人 000191076

新日鉄ソリューションズ株式会社

東京都中央区新川2丁目20番15号

(72) 発明者 下村 修

東京都千代田区大手町2丁目6番3号 新

日本製鐵株式会社内

(72) 発明者 酒井 秀典

東京都千代田区大手町2丁目6番3号 新

日本製鐵株式会社内

(74) 代理人 100091269

弁理士 半田 昌男

Fターム (参考) 5B017 AA07 BA05 CA16

5B075 KK42 KK54 KK63 UU05

(54) 【発明の名称】 ドキュメント管理システム

(57) 【要約】

【課題】 必要なドキュメントに対して必要なときに迅速にアクセスでき、かつ、さまざまなセキュリティレベルに応じて確実にアクセスを制限する。

【解決手段】 図2に示したアクセスコントロールリストは、ドキュメントへのアクセスを制限する際の中心的な役割を果たす。アクセスコントロールリストの一つの行は、各列の先頭行に記載された複数のフィールドから構成される。一つの行 (レコード) に含まれる各フィールドの情報が、ある一つの文字列を含むドキュメントに対して所定のアクセス制限を設定するのに必要とされる情報の全体である。「文字列」フィールドは、データベースに蓄積されている多数のドキュメントのうち、このフィールドに記載されている文字列を含むドキュメントが、アクセスを制限される対象となるドキュメントであることを意味する。

ID	文字列	アクセス可能者	アクセスレベル	有効期限	有効期限後レベル
	「ABC」	甲村 太郎	3	2000/09/30	1
	「CDE」	乙野 次郎	3	2000/09/30	1
	「GHIJ」	丙井 三郎	2	2000/09/30	1
	「KLM」	丁野 四郎	1	2000/09/30	0
⋮	⋮	⋮	⋮	⋮	⋮

## 【特許請求の範囲】

【請求項 1】 登録されたドキュメントについて、ユーザーからのアクセスを制限するドキュメント管理システムにおいて、

登録しようとするドキュメントに特定のデータが含まれている場合は、当該ドキュメントに対し、少なくとも前記データが含まれているアクセス制限情報を付与して登録し、後に当該ドキュメントに対してアクセス要求があったときは、付与されているアクセス制限情報の内容に従って、アクセスを制限することを特徴とするドキュメント管理システム。

【請求項 2】 前記アクセス制限情報には、前記データの他に、当該ドキュメントに対するアクセスをどのように制限するかを示す情報を含んでおり、当該ドキュメントに対してアクセスが要求されたときは、当該情報を参照してアクセスの制限の仕方を決定することを特徴とする請求項 1 記載のドキュメント管理システム。

【請求項 3】 登録しようとするドキュメントに前記特定のデータが含まれているかどうかの判定は、当該ドキュメントを登録するとき、前記アクセス制限情報を登録するとき、又は、当該ドキュメントに対してアクセス要求があったときのいずれかであることを特徴とする請求項 1 又は 2 記載のドキュメント管理システム。

【請求項 4】 前記アクセス制限情報は、制限付きでアクセスを許されるものを特定する情報を含んでいることを特徴とする請求項 1 乃至 3 のうちいずれか一項記載のドキュメント管理システム。

【請求項 5】 前記アクセス制限情報は、アクセス制限が適用される有効期限を含んでいることを特徴とする請求項 1 乃至 4 のうちいずれか一項記載のドキュメント管理システム。

【請求項 6】 前記アクセス制限情報は、複数のフィールドからなる一つのレコードの形態で用意され、かつ、当該レコードを特定するための ID 情報を含んでおり、ドキュメントに対する前記レコードの付与は、ドキュメントに対して当該 ID 情報を関連付けることによって行うことを特徴とする請求項 1 乃至 5 のうちいずれか一項記載のドキュメント管理システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、さまざまなレベルでセキュリティを確保したい多くのドキュメントを管理するドキュメント管理システムに関する。

## 【0002】

【従来の技術】企業、大学、官公庁などでは、各部署において作成された各種資料、文書、図面などの大量のドキュメントをコンピュータによって一括管理し、必要な場合には、関連する文書を迅速に検索して再利用（アクセス）することができるようにしたドキュメント管理システムが実用化されている。

## 【0003】

【発明が解決しようとする課題】しかし、これらのドキュメントの中には、一般に公表してもよいものから社内特定の者以外の目には触れさせたくないもの、あるいは、単なる参照は認めるが印刷までは認めないられないもの、内容の改変を認めてもよいものから一切の改変を認めるべきでないものまで、さまざまなセキュリティレベルのドキュメントが含まれる。大量のドキュメントが蓄積されている場合に、アクセスが要求された段階で、そのドキュメントがどのようなセキュリティレベルなのかを判断し、それに基づいてアクセスを制限するようにしていたのでは、必要なドキュメントに対して必要なときに迅速にアクセスできるというドキュメント管理システム本来の利点が失われる。

【0004】本発明は、上記事情に基づいてなされたものであり、その目的は、必要なドキュメントに対して必要なときに迅速にアクセスでき、かつ、さまざまなセキュリティレベルに応じて、確実にアクセスを制限することができるドキュメント管理システムを提供することである。

## 【0005】

【課題を解決するための手段】上記の目的を達成するために、請求項 1 記載の発明は、登録されたドキュメントについて、ユーザーからのアクセスを制限するドキュメント管理システムにおいて、登録しようとするドキュメントに特定のデータが含まれている場合は、当該ドキュメントに対し、少なくとも前記データが含まれているアクセス制限情報を付与して登録し、後に当該ドキュメントに対してアクセス要求があったときは、付与されているアクセス制限情報の内容に従って、アクセスを制限することを特徴とする。

【0006】請求項 2 記載の発明は、請求項 1 記載のドキュメント管理システムにおいて、前記アクセス制限情報には、前記データの他に、当該ドキュメントに対するアクセスをどのように制限するかを示す情報を含んでおり、当該ドキュメントに対してアクセスが要求されたときは、当該情報を参照してアクセスの制限の仕方を決定することを特徴とする。

【0007】請求項 3 記載の発明は、請求項 1 又は 2 記載のドキュメント管理システムにおいて、登録しようとするドキュメントに前記特定のデータが含まれているかどうかの判定は、当該ドキュメントを登録するとき、前記アクセス制限情報を登録するとき、又は、当該ドキュメントに対してアクセス要求があったときのいずれかであることを特徴とする。

【0008】請求項 4 記載の発明は、請求項 1 乃至 3 のうちいずれか一項記載のドキュメント管理システムにおいて、前記アクセス制限情報は、制限付きでアクセスを許されるものを特定する情報を含んでいることを特徴とする。

【0009】請求項5記載の発明は、請求項1乃至4のうちいずれか一項記載のドキュメント管理システムにおいて、前記アクセス制限情報は、アクセス制限が適用される有効期限を含んでいることを特徴とする。

【0010】請求項6記載の発明は、請求項1乃至5のうちいずれか一項記載のドキュメント管理システムにおいて、前記アクセス制限情報は、複数のフィールドからなる一つのレコードの形態で用意され、かつ、当該レコードを特定するためのID情報を含んでおり、ドキュメントに対する前記レコードの付与は、ドキュメントに対して当該ID情報を関連付けることによって行うことを特徴とする。

【0011】

【発明の実施の形態】以下に、図面を参照して、本発明の実施の一形態について説明する。図1は、本発明に係るドキュメント管理システムを実施するためハードウェア構成の一例を示している。同図に示すように、本実施形態のドキュメント管理システム10では、ネットワーク20に、サーバー端末21及びクライアント端末22<sub>1</sub>、22<sub>2</sub>、…、22<sub>n</sub>が接続されており、さらに、サーバー端末21にはデータベース23が接続されている。ここで、ネットワーク10として利用可能なものには、インターネットの他、LAN、WANその他が含まれる。また、一例として、サーバー端末21としては、ワークステーションあるいはメインフレームを、クライアント端末22<sub>1</sub>、22<sub>2</sub>、…22<sub>n</sub>としては、ワークステーションあるいはパーソナルコンピュータを利用することができる。

【0012】本実施形態のドキュメント管理システム10は、サーバー端末21の管理のもとにデータベース23に蓄積されているドキュメントに対して、クライアント端末22<sub>1</sub>、22<sub>2</sub>、…22<sub>n</sub>からユーザーがアクセスを要求してきたときに、当該ドキュメントについてアクセス制限の設定がなされている場合には、そのアクセス制限の内容に応じて、当該ドキュメントの一部又は全部について当該ユーザーによるアクセスを制限することによって、重要なドキュメントについて十分なセキュリティを確保することを目的とする。

【0013】ここで、「アクセス」とは、ユーザーが、データベース23に蓄積されている特定のドキュメントを参照すること、印刷すること、他の媒体に複写すること、ドキュメントの内容を改変することなどを含んでいる。また、「アクセスを制限する」とは、特定のドキュメントについての参照、印刷、複写、改変などを、部分的あるいは全体的に禁止することを意味する。さらに、「アクセス制限の設定」とは、後述のように、データベース23に登録されるドキュメントに対し所定のID情報を付与することによって、ユーザーからのアクセスを制限することをいう。

【0014】本実施形態のドキュメント管理システム1

0では、図2にそのフォーマットの一例を示す「アクセスコントロールリスト」が、ドキュメントへのアクセスを制限する際の中心的な役割を果たす。このアクセスコントロールリストは、サーバー端末21上に格納されている。アクセスコントロールリストは、本システムを運用する上で必須のものであるが、運用してゆくに従って、その内容は徐々に変化してゆく。

【0015】図2に示したアクセスコントロールリストにおいて、一つの行は、各列の先頭行に記載された複数の項目（以下「フィールド」という）から構成される。一つの行に含まれる各フィールドの情報（以下「レコード」という）が、ある一つの文字列を含むドキュメントに対して所定のアクセス制限を設定するのに必要とされる情報の全体である。

【0016】図2において、「文字列」フィールドは、データベース23に蓄積されている多数のドキュメントのうち、このフィールドに記載されている文字列を含むドキュメントが、アクセスを制限される対象となるドキュメントであることを意味する。したがって、後述のように、あるドキュメントを本システムのデータベース23に登録する際には、そのドキュメントの中に図2の「文字列」フィールドに記載された文字列が含まれているかどうかについて、サーバー端末21上で検索が実行される。なお、ここでは説明を分かり易くするために「文字列」と呼んでいるが、これはビット列などのデータ列であってもよいことは勿論である。

【0017】「アクセス可能者」フィールドには、その「文字列」を含むドキュメントについて、制限付きのアクセスが認められる者を特定するための情報が記載される。この情報は、図2に例示したように、人名を一つあるいは二つ以上羅列するといった形式でもよいし、「経理部」、「人事部」、「開発部」などといった会社内における組織の名称であってもよいし、「課長以上」、「部長以上」、「取締役以上」といった会社組織内での役職名などで記載する形式を採用してもよい。あるいは、これらの一部又は全部を複合した形式でもよい。組織名や役職名のような総括名称の場合には、それらの総括名称に該当する個々の者がアクセス可能者となる。なお、アクセス可能者を特に限定せず、すべてのユーザーに対して同じようにアクセス制限を行う場合には、「アクセス可能者」フィールドは必須のものではない。

【0018】「アクセスレベル」フィールドは、前述の「文字列」フィールドに記載された文字列が含まれるドキュメントに対して、どのような態様でアクセスを制限するかを指定するフィールドである。言い換えると、それぞれのドキュメントに対するセキュリティレベルを指定するフィールドである。

【0019】図3は、「アクセスレベル」フィールドに記載されるアクセスレベルの内容とそれらを指し示すための記号を、表にして示したものの一例である。同図のレ

ベル分けに従ってアクセスレベルを設定する場合について説明する。ある文字列についてアクセスレベルとしてレベル3が付与されていれば、その文字列を含むドキュメントについては、その全体について一切の参照が禁止され、改変や印刷も禁止される。レベル2が付与されていれば、ディスプレイ画面上で参照することは可能だが、印刷や改変は禁止される。レベル1が付与されていれば、参照、印刷とも可能だが、改変は禁止される。さらに、レベル0が付与されていれば、参照、印刷、改変は認められるが、ドキュメントの削除は禁止される。

【0020】アクセスレベルの指定の仕方には、図3のような態様以外にも種々のものが考えられる。図3では、主としてドキュメントへのアクセスの仕方という観点からアクセスレベルを指定しているが、これ以外にも、たとえばドキュメントのどの部分についてアクセスを制限するかという観点からアクセスレベルを指定することもできる。すなわち、「文字列」フィールドに記載されている文字列を含むドキュメントについては、その表紙だけを参照可能にするとか、「文字列」フィールドに含まれる文字列が記載されているページだけは参照できないようにするとか、あるいは当該文字列の部分だけを黒塗りにして表示するといった方法である。あるいはまた、会社であれば、社内のトップしか参照できないレベル、部長級以上しか参照できないレベル、課長級しか参照できないレベル、社員全員が参照できるレベル、そして社外の者に公表してもよいレベル、といったように、「アクセスが許される者」という観点からアクセスレベルを設定することも可能である。

【0021】また、ある化合物名の文字列を含むドキュメントについてアクセス制限を行い、さらにその中で、たとえば当該化合物の具体的な成分比が記述されているドキュメントについてはより高いアクセス制限を加えて、アクセスできる者の範囲をより狭く限定するといったように、一つのレコード内でアクセスレベルを複数段階に設定することもできる。これとは逆に、ある文字列を含むドキュメントに対し、「アクセス可」、「アクセス不可」というように二つだけの単純なレベル分けを採用することもできる。このように、アクセスレベルの指定の仕方には特に制限はなく、それぞれの実施の形態に応じて相応しい方法を選択すればよい。

【0022】図2に示したアクセスコントロールリストのうち、「有効期限」フィールドは、「アクセスレベル」フィールドで指定されたアクセスレベルが有効である期間の末日を指定するフィールドである。図2の例では、文字列「ABC」のレコードの「有効期限」フィールドには「2000年9月30日」と記載されているが、これにより、文字列「ABC」についてアクセスレベルを「3」にしておく期間が、2000年9月30日までであることが指定されている。

【0023】このようにアクセスレベルの有効期限を指

定することが必要となる状況としては、例えば、文字列「ABC」がある製品の開発プロジェクトの名称、あるいは製品開発コードであって、その製品発表が2000年10月1日であるような場合に、9月30日まではたとえ社内であっても文字列「ABC」が含まれているドキュメントについては、それを見ることができる者の範囲を狭く限定しておきたいというような場合が該当する。図2の例では、この期間が経過した後は、次の「有効期限後レベル」フィールドに指定されているように、アクセスレベルを「1」に下げてアクセス制限が緩和されている。「有効期限後レベル」フィールドにアクセスレベルを指定しなければ、その文字列を含むドキュメントに対するアクセス制限はなくなる。

【0024】この「有効期限」フィールドも、必ずしも一つだけとは限らず、有効期限を複数設定できるようにしてもよい。この場合は、それぞれの「有効期限」を経過するたびに、そのドキュメントへのアクセスを制限するアクセスレベルは、段階的に変化する。

【0025】なお、通常は、図2の例のように有効期限を過ぎたときは、その文字列を含むドキュメントに対するアクセスレベルを低く指定しておく場合が多い。しかし、状況によっては、ある時期を経過した後にアクセスレベルをそれ以前よりも高くしたいと考える場合もある。

【0026】たとえば、あるコンピュータソフトウェアのバージョンアップ製品を2000年10月1日に発売することになっており、それ以降は旧バージョンの製品は販売しないことが決まっているとすると、新旧両バージョンの操作マニュアルがドキュメントとしてデータベース23に蓄積されており、9月30日までは旧バージョンの操作マニュアルを使用するが、10月1日以降は新バージョンの操作マニュアルに切り替えるものとする。このような場合に、旧バージョンの操作マニュアルに関するドキュメントについては「有効期限後レベル」フィールドのアクセスレベルを高くして、10月1日以降は特別な場合を除いて参照できないようにしておけばよい。このようにすると、新バージョンのマニュアルと旧バージョンのマニュアルを取り違えたり、バージョンアップ製品の発売後に社外の顧客に誤って旧バージョンのマニュアルが配布されるといった事態を未然に防止できる。

【0027】別の例として、ある化学品又は医薬品の製造方法について一般的な製法が記述されているドキュメントがあり、このドキュメントに基づいて新製品を開発するプロジェクトがあったとする。そして、開発過程において徐々に詳しい成分比などを決めてゆきながら実験を繰り返し、その結果を逐次上記ドキュメントに追加記載してゆくことか決まっていたとする。この場合、最初に立案された予定によれば、ある日時以降は具体的な成分比を用いた実験が開始されることになっているような

場合には、その日時以降は、アクセスレベルをより高くして、社内ユーザーからのアクセスに対する制限を強化する必要がある。このような場合も、「有効期限後レベル」フィールドのアクセスレベルを高くする必要がある事例の一つである。

【0028】このように、アクセスレベルについて「有効期限」という概念を導入することによって、同じ一つのドキュメントあるいは同じ一つの文字列についても、アクセス制限の内容をダイナミックに変化させることができる。

【0029】図2において、各行の左端に設けられている「ID」フィールドは、それぞれのレコードを特定するためのID情報が記載されるフィールドである。したがって、ここに記載されるID情報は、各レコードを一意的に特定できるものである必要がある。たとえば、あるドキュメント内に、図2のアクセスコントロールリスト1行目の「ABC」という文字列が存在したことが分かった場合には、そのドキュメントには、登録の際に、1行目のレコードのIDフィールドに記載されているID情報が付与される。このID情報が付与されたことによって、そのドキュメントに対してアクセス制限が設定されたことになる。

【0030】一つのドキュメントに対して、複数のアクセス制限が設定されることもある。例えば、あるドキュメント内に「ABC」という文字列だけでなく、「CDF」という文字列も含まれていたような場合には、そのドキュメントには、図2の1行目のレコードを特定するID情報と2行目のレコードを特定するID情報が付与され、これにより二つのアクセス制限が設定されたことになる。

【0031】上述のように、図2の「文字列」フィールドに登録されている文字列がキーワードとなってドキュメントに対するアクセスが制限されるので、ある範囲のドキュメントへのアクセスを確実に制限するためには、それらに含まれる文字列を、確実にアクセスコントロールリストに登録しておくことが必要となる。そこで、一例として次のような方法によって、重要なドキュメントに対するアクセスを制限する。

【0032】ある企業においてあるプロジェクトが発足し、このプロジェクトに関連するドキュメントについては、すべて一定のアクセスレベルでアクセスを制限することか決められたとする。このような場合には、関連するすべてのドキュメントの任意の位置、あるいは予め合意された所定位置に、そのプロジェクト名や暗号など、予め決められた文字列を必ず記載しておくことを申し合わせる。それと同時に、当該文字列を「文字列」フィールドに記載したレコードを作成し、図2に示したアクセスコントロールリストに登録する。このような準備を行った上で、このプロジェクトに関連するすべてのドキュメントを図1のデータベース23に登録する。このよう

にしておけば、当該プロジェクトの関係者は必要な時にいつでもこれらのドキュメントにアクセスすることができ、これら以外の者がアクセスしようとしたときには、アクセスコントロールリストに登録されたアクセスレベルの内容に応じてアクセスを制限することができ、利便性とセキュリティの高さを両立させることができる。

【0033】次に、アクセスを制限しようとするドキュメントを本実施形態のシステムに登録する際の手順について、図4のフローチャートを参照しながら説明する。この場合は、図2に示すようなアクセスコントロールリストが、既にサーバー端末21上に用意されているものとする。

【0034】あるドキュメントに登録しようとする、システムはまず、サーバー端末21上において、予め用意されている図2のアクセスコントロールリストの「文字列」フィールドに登録されている文字列のそれぞれについて、当該ドキュメントを対象として順番に検索を実行する(ステップ10)。この検索の結果、そのドキュメントに図2の「文字列」フィールドに登録されている文字列が含まれていた(ヒットしたら)(ステップ11)、そのドキュメントに、その文字列が含まれるレコードのID情報を付与して(ステップ12)、データベース23に登録する(ステップ13)。これによって、当該ドキュメントには、アクセス制限が設定される。一つのドキュメントに、図2に登録されている文字列が複数含まれていることもあるので、その場合は一つのドキュメントに複数のID情報が付与され、複数のアクセス制限が設定される。

【0035】同様の処理を全ての文字列について行う(ステップ14)、アクセスコントロールリストに登録されている文字列が、登録しようとするドキュメントの一つも含まれていない場合には、当該ドキュメントにはID情報は付与されないで、すなわちアクセス制限が設定されない状態で、データベース23に登録される(ステップ15)。

【0036】次に、上記のようにして本システムのデータベース23に登録されたドキュメントに対してアクセスが要求された場合の処理手順について、図5に示したフローチャートを参照しながら説明する。あるユーザーが本システムを利用しようとする場合には、まず、そのユーザー自身がこのシステムを利用する権限を有するものであるか否かの判定を行う(ステップ20)。この判定方法としては、ユーザーに対して自己認証のためのIDコードやパスワードなどの入力を求め、これをサーバー端末21が別途設けられている社員データベースなどを参照して、本人であるか否かを認証するという方法が一般的である。

【0037】当該ユーザーが本システムを利用する権限を有する者とであると判定された場合には、次に、そのド

キュメントがデータベース23に登録されているものであるかを判定する(ステップ21)。この判定において、ユーザーがアクセスしようとするドキュメントを特定する方法として、文書名、作成者名、文書番号などの属性情報に基づいて検索するようにしてもよいし、ユーザーがキーワードを入力し、その文字列を含むかどうかを全ドキュメントに対して全文検索を実行するようにしてもよい。あるいはまた、データベース23にファイルが階層構造的に格納されている場合には、GUIとしてフォルダツリーを表示し、ユーザーがこのツリーを上位の階層から下位の階層に向かって探索して行き、希望するファイルが見つかった段階でそのファイル名をクリックするなどしてドキュメントを選択するという方法を採用してもよい。

【0038】その結果、データベース23に該当するドキュメントが登録されていない場合には、ユーザーに対してその旨を表示する(ステップ22)。一方、データベース23に該当するドキュメント、あるいはユーザーが探索していたドキュメントがデータベース23に登録されている場合には、そのリストを端末の画面上にリスト表示し(ステップ23)、ユーザーに対して、アクセスしようとしているドキュメントを選択するよう促す。続いて、選択されたドキュメントについて、図2に示したアクセスコントロールリストのレコードを指定するID情報が付与されているかどうかをチェックする(ステップ24)。ID情報が付与されていない場合は、そのドキュメントにはアクセス制限が設定されていないので、その場合は、参照、印刷、改変など、ユーザーが希望する態様で利用できるよう、そのドキュメントのデータをユーザーに提供する(ステップ25)。

【0039】一方、当該ドキュメントにID情報が付与されている場合は、まず、認証されたユーザーが「アクセス可能者」フィールドに記載された者の中に含まれているかを判定する(ステップ26)。「アクセス可能者」の範囲に含まれていない場合は、この時点でアクセスを拒否する(ステップ27)。一方、当該ユーザーが「アクセス可能者」に含まれている場合には、現在の日時と有効期限とを比較対照し、現在の時点で適用すべきアクセスレベルを決定する(ステップ28)。そして、この決定されたアクセスレベルに基づいて制限された内容で、当該ドキュメントを当該ユーザーの利用に供するための処理を行う(ステップ29)。

【0040】なお、当該ドキュメントに複数のID情報が付与されていて、そのいずれの「アクセス可能者」フィールドにも当該ユーザーが含まれていた場合には、予め決められたアルゴリズムに従って、例えば、より高いアクセスレベルに基づいてアクセスを制限するなどの処理を行う。

【0041】次に、アクセスコントロールリストに新たなレコードが追加された場合の処理について説明する。

企業活動などが活発になれば、それだけ秘匿しておきたいドキュメントも増えると考えられるので、そのような場合には、アクセスコントロールリストに新たなレコードが追加される機会も増えると考えられる。このように、新たなレコードをアクセスコントロールリストに追加する場合には、新たなレコードが追加されるたびに、そのレコードに含まれる文字列について、すでにデータベースに登録されている全てのドキュメントを対象として全文検索を行う。そして、当該文字列が含まれているドキュメントが見つかったならば、そのドキュメントに対して、当該文字列に関連するレコードに基づいてアクセス制限の設定を行う。これにより、既に登録されているドキュメントであっても、あとから追加されたレコードによってアクセス制限の対象とすることができる。

【0042】所定のドキュメントに対するアクセス制限を会場する場合には、次のようにする。たとえば、ある社内プロジェクトの名称が「文字列」フィールドに記載されているレコードが登録されており、このプロジェクトが終了したので、このプロジェクトに関連するドキュメントへのアクセス制限を解除したい考えたとする。この場合は、予めこのレコードを登録する際に、プロジェクトが終了する日時を「有効期限」フィールドに指定しておき、「有効期限後レベル」の値を制限がないことを示す値にしておくか、あるいは、アクセス制限が不要となった段階で、アクセスコントロールリストから当該レコードを削除する。この場合、当該レコードがまったく不要なものとなった場合には、後者の方法を採用の方が望ましい。その理由は、レコードそのものが削除されていれば、新たなドキュメントを登録するときの文字列検索を実行する際に、当該レコードの「文字列」フィールドに記載されていた文字列については検索を行わずに済み、その分、処理時間を短縮できるからである。

【0043】アクセス制限を解除する別の方法として、予めアクセスコントロールレベルに「無効日時」というフィールドを設けておき、ここに日時が設定されている場合には、その日時以降は当該レコードは無効なレコードと認定し、その後に新たなドキュメントが登録されるときでも、そのレコードに含まれる文字列については検索を行わない、という方法を採用することもできる。このようにしおけば、レコードそのものを削除する場合と同程度の処理時間の短縮が図られる上に、過去にどのような内容のレコードが存在したかという履歴を、のちに調べることが可能となる。

【0044】すでに、図4に示したフローチャートとの関連で説明したように、あるドキュメントを本実施形態のドキュメント管理システムに登録する際に、アクセスコントロールリストに登録されている文字列の検索を行って、そのドキュメント中にアクセスコントロールリストに登録されている文字列が含まれているかどうかを判定し、この段階で各ドキュメントに各レコードのID情



報を付与する、というのが本システムの基本的な利用方法である。これに対して、単に利用のし易さだけを考慮して、利用の制限については特に考えずにドキュメントの蓄積を行ってきたデータベースが既に存在しており、ある時点から、このようなデータベースについても本実施形態のシステムを適用としてアクセス制限を設定したいという要求が生じる場合がある。このような場合には、次の手順によって、既存のデータベースに対して、本実施形態のドキュメント管理システムを適用する。

【0045】まず、アクセスコントロールリストを作成する。これには最低限一つのレコードが登録されていることが必要となる。アクセスコントロールリストが作成されたら、データベースにアクセスし、既に蓄積されているドキュメントを一つ呼び出し、アクセスコントロールリストに登録されているすべての文字列について順番に検索を行う。そして、そのドキュメント内に、アクセスコントロールリストに登録されている文字列が見つかった場合には、そのレコードを特定するID情報を当該ドキュメントに付与してアクセス制限を設定する。次に、別のドキュメントを呼び出して、同様の処理を行う。以下、同様にして、データベースに蓄積されているすべてのドキュメントに対して、同様の処理を行うことによって、既存のデータベースに対して本実施形態のシステムを適用し、必要なドキュメントに対してアクセスを制限できるようになる。

【0046】このような処理の実行には、特にデータベースの規模が大きくなるとかなりの時間を要し、その間はデータベースを他の目的に利用できなくなる。しかし、このような処理を実行しなければならないのは、システム導入当初における最初の一回だけであり、また、データベースの利用が少ない、例えば夜間などに実行するようにすれば、業務への影響は最小限に抑えられる。

【0047】また、一時的にでもデータベースが利用できなくなるのを避けたい場合には、上記のように蓄積されているすべてのデータについて一括して登録処理を行う代わりに、あるドキュメントに対してアクセスが要求された場合に、その都度、アクセスコントロールリストに登録されている文字列が含まれているかどうかを判定し、含まれていたらその段階で当該文字列のID情報を付与するようにしてもよい。このようにすれば、まだシステムへの登録が済んでないドキュメントに対してアクセスが要求された場合に、アクセスが許されるか否かを判定するまでに多少の時間はかかるが、システム導入当初において、すべてのドキュメントを一括して登録処理を行う場合に必要となる長時間の処理は不要となる。

【0048】ところで、後者のような方法が可能であるならば、既に導入されている本システムにドキュメントを登録する場合においても、その時点ではアクセスコントロールリストに登録されている文字列が含まれているかどうかの判定を行わずに、そのドキュメントに対して

アクセスが要求された時点でアクセスコントロールリストに登録されている文字列が含まれているかどうかを判定することも可能であろうと考えられる。

【0049】しかしながら、そのようにすると、例えばアクセスコントロールリストに登録されているレコードの数が非常に多いような場合（一例として1000レコード分ある場合）には、あるドキュメントに対してアクセスを要求すると、そのたびにこの1000個のレコード内の文字列について、それぞれがアクセス要求したドキュメントに含まれているかどうかを検索しなければならないことになり、結果が出るまでに非常に長い時間を必要とする。このため、業務の効率を考えた場合には、ドキュメントに対してアクセスが要求された時点ですべてのレコード内の文字列についてそれらが当該ドキュメントに含まれているかどうかを検索するという方法は、既に蓄積されている大量のドキュメントについて後から本システムを導入するという例外的な場合を除いて、望ましい方法とは言えない。

【0050】以上の説明から明らかなように、本実施形態に係るドキュメント管理システムは、社内や社内に対して秘匿しておきたい情報を扱う企業でのドキュメント管理や、官公庁などにおいて大量のドキュメントについて様々なレベルでセキュリティを確保したいという場合などに有用である。

【0051】以上、本発明の実施の一形態について説明してきたが、本発明は上記実施形態に限定されるものではなく、その要旨の範囲内において種々の変更が可能であり、それらも本発明の技術的範囲に含まれることはいうまでもない。

【0052】

【発明の効果】以上説明したように、本発明によれば、ドキュメントを登録する際に、すなわち、ドキュメントに対してアクセスを実行するよりも前に、事前にアクセス制限情報を付与して登録しておくので、アクセスの際には、迅速に、そのドキュメントがどのような態様でアクセスを制限されているのかをシステムが判断し、その結果に基づいてアクセスが制限される。このため、必要なドキュメントに対して必要なときに迅速にアクセスできるという利点を維持しつつ、さまざまなセキュリティレベルに応じて、確実にアクセスを制限することができる。

【図面の簡単な説明】

【図1】本発明に係るドキュメント管理システムを実施するためハードウェア構成の一例を示した図である。

【図2】ドキュメントに対するアクセス制限を実行する際に中心的な役割を果たすアクセスコントロールリストのフォーマットの一例を示した図である。

【図3】アクセスレベルフィールドに記載されるアクセスレベルの内容とそれらを指し示すための記号を表にして示したもの一例である。



【図4】アクセスを制限しようとするドキュメントをシステムに登録する際の手順を示したフローチャートである。

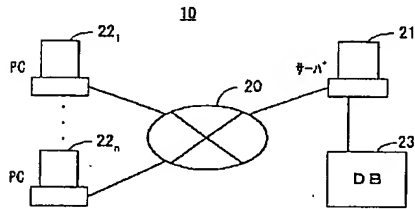
【図5】データベースに登録されたドキュメントに対してアクセスが要求された場合の処理手順を示したフロー\*

\*チャートである。

【符号の説明】

10…ドキュメント管理システム、20…インターネット、21…サーバ端末、22<sub>1</sub>、22<sub>2</sub>、…、22<sub>n</sub>…クライアント端末、23…データベース

【図1】



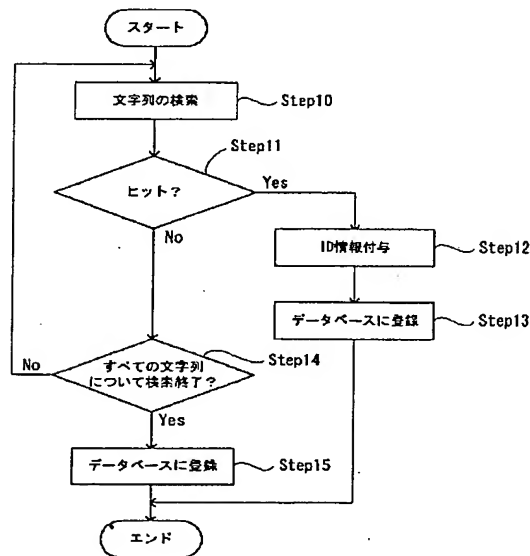
【図2】

ID	文字列	アクセス可能者	アクセスレベル	有効期限	有効期限後レベル
	「ABC」	甲村 太郎	3	2000/09/30	1
	「CDE」	乙野 次郎	3	2000/09/30	1
	「GHI」	丙井 三郎	2	2000/09/30	1
	「KLM」	丁野 四郎	1	2000/09/30	0
⋮	⋮	⋮	⋮	⋮	⋮

【図3】

アクセスレベル	内容
3	参照不可
2	参照のみ
1	印刷可
0	改変可

【図4】



【図5】

